The Art of Wireless War

KCCMG Impact Conference

Fall 2004

Sprint Proprietary

Thoughts From An Ancient Master

"The general who wins a battle makes many calculations in his temple before the battle is fought.“ Sun Tzu, *The Art of War*

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu, *The Art of War*

Wireless LAN Usage Is Growing

"The percentage of companies spending more than $10,000 annually [on WLAN deployments] will grow from 26 percent in 2003 to 35 percent in 2004."

Julie Ask, Jupiter Research

Security Remains A Big Concern

Although 84 percent of companies have not had their WLAN breached, "security is the top barrier, cited by nearly half of all companies" as the reason they are not deploying or expanding Wi-Fi networks.

Understanding Corporate WLAN Architecture Choices, Jupitermedia

IEEE Standards “decoder ring”

802.11a	5GHz OFDM PHY
802.11b	2.4GHz CCK PHY
802.11c	802.11 bridging
802.11d	International roaming
802.11e	QoS/efficiency enhancements
802.11F	Inter AP protocol
802.11g	2.4GHz OFDM PHY
802.11h	5GHz regulatory extensions
802.11i	Security enhancements
802.11j	Japan 5GHz band extensions
802.11k	Radio resource measurement
802.11l	Skipped (typographically unsound)
802.11m	Maintenance
802.11n	High throughput PHY

Typical WLAN Configuration

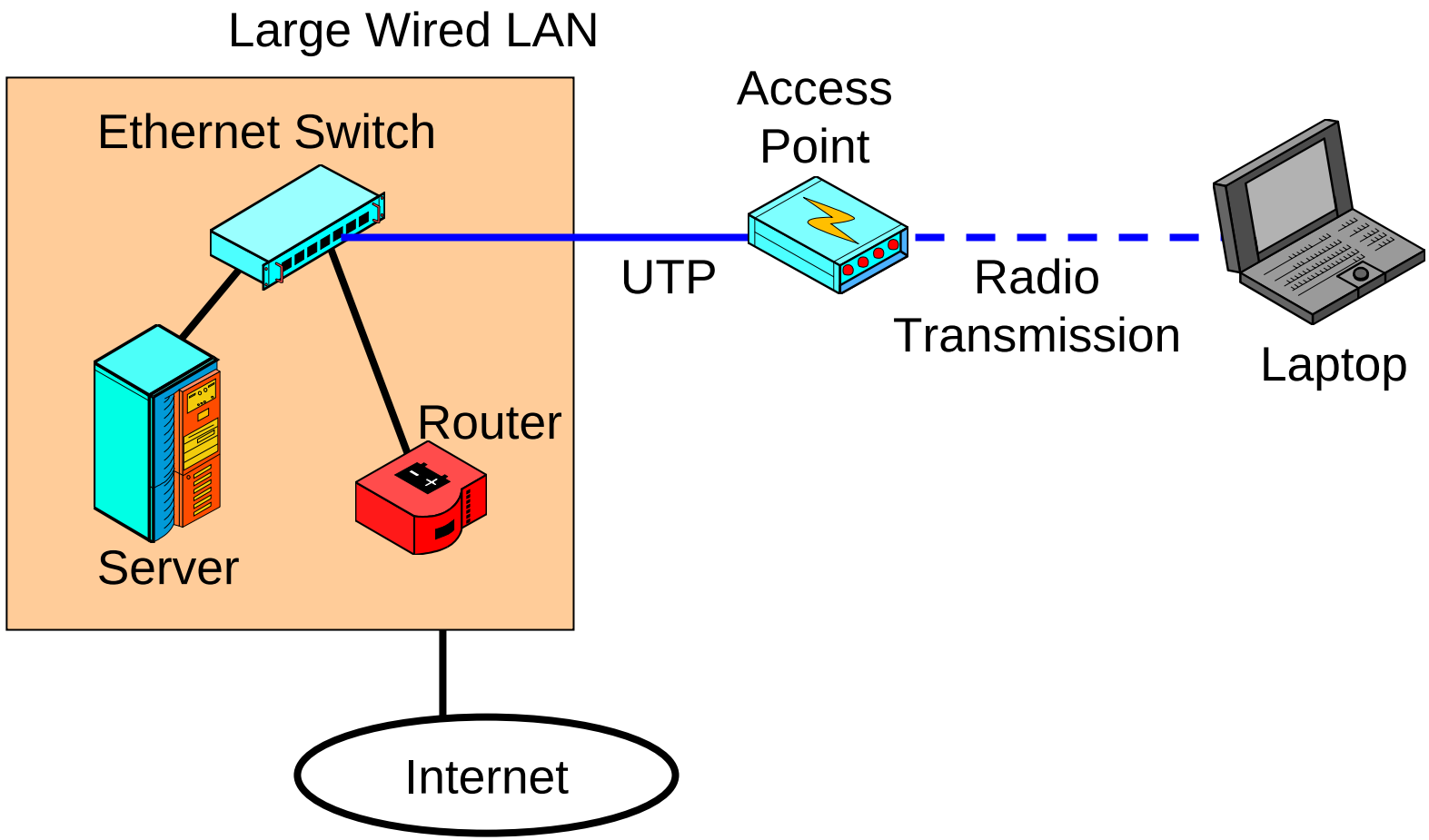


Diagram Courtesy of Intel Corp.

802.11 Security Threats

- Drive-By Insecurity
  - Traffic captured from outside the enterprise
  - Traffic “injected” into the enterprise

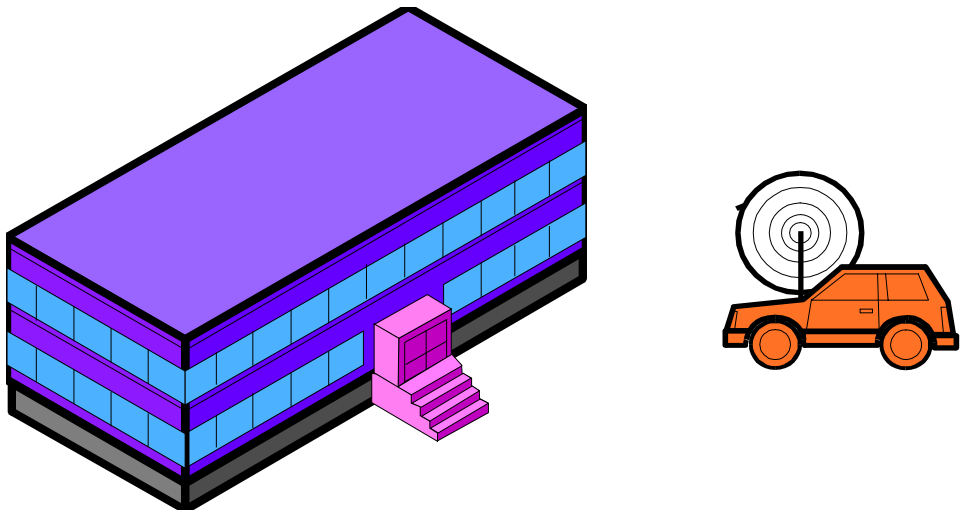


Diagram Courtesy of Intel Corp.

802.11 Security – The Early Years

- **Wired Equivalent Privacy (WEP)**
  - **Initial security method for 802.11 devices**
  - **All stations share the same encryption key with the access point**
  - **This key is rarely changed**
  - **Shared static keys means that a large volume of traffic is encrypted with the same key**
  - **With so much traffic generated with one unchanging key, cryptanalysts were able to crack the key by collecting data for a few days**

Know Your Enemy

- **Who**
  - **Thrill Seekers - Access Thieves**
  - **Identity Thieves**
  - **Data Thieves**

Know Your Enemy

- How / Equipment
  - Laptop / PDA
  - Wireless card + Antenna
  - OS (sometimes Windows, usually Linux)
  - Software Tools
    - Netstumbler
    - Ethereal
    - WEPCrack

Wireless Tools

Aerosol	http://www.stolenshoes.net/sniph/aerosol.html
Airfart	http://airfart.sourceforge.net/
AirJack	http://802.11ninja.net/airjack/
Airscanner Mobile Sniffer	http://www.airscanner.com/downloads/sniffer/sniffer.html
AirSnarf	http://airsnarf.shmoo.com/
AirSnort	http://airsnort.shmoo.com/
AirTraf	http://www.elixar.com/corporate/history/airtraf-1.0/
anwrap	http://www.securiteam.com/tools/6O00P2060I.html
AP Hopper	http://aphopper.sourceforge.net/
AP Radar	http://apradar.sourceforge.net/
APhunter	http://www.math.ucla.edu/%7Ejimc/mathnet_d/download.html
APSniff	http://www.bretmounet.com/ApSniff/
APTools	http://winfingerprint.sourceforge.net/aptools.php
Asleap	http://asleap.sourceforge.net/
BSD-AirTools	http://www.dachb0den.com/projects/bsd-airtools.html
ClassicStumbler	http://homepage.mac.com/alk/classicstumbler.html
DMZS-Carte	http://www.dmzs.com/tools/files/wireless.phtml
dstumbler	http://www.dachb0den.com/projects/dstumbler.html
dweputils	http://www.dachb0den.com/projects/dweputils.html
Ethereal	http://www.ethereal.com/

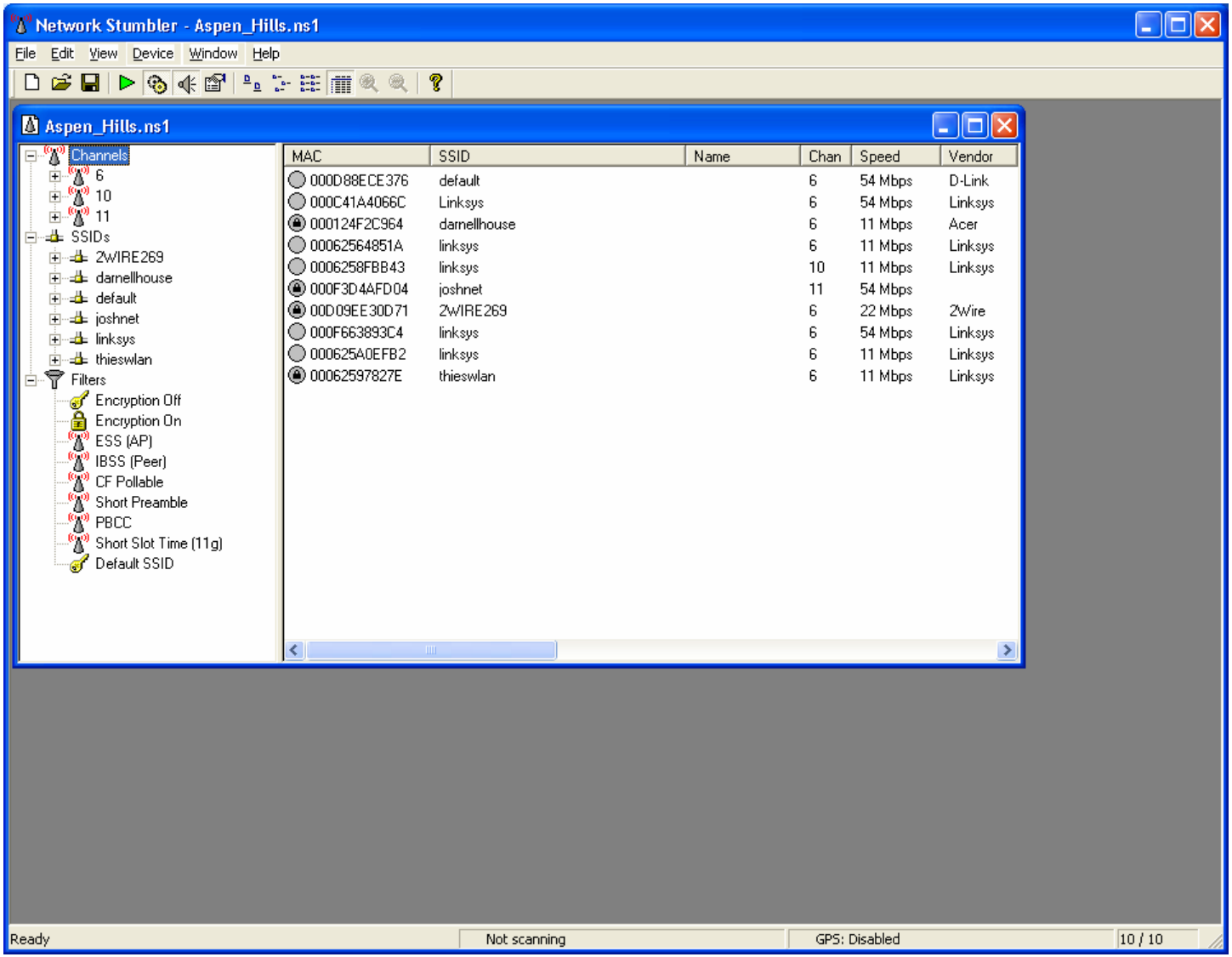
Wireless Tools (cont.)

FakeAP	http://www.blackalchemy.to/project/fakeap/
gpsd	http://freshmeat.net/projects/gpsd/
Hotspotter	http://www.remote-exploit.org/codes.html
iStumbler	http://www.istumbler.net/
KisMAC	http://www.binaervarianz.de/projekte/programmieren/kismac/
Kismet	http://www.kismetwireless.net/
LibRadiate	http://www.packetfactory.net/projects/libradiate/
LibWnet	http://www.dachb0den.com/users/h1kari/work/.0-day/bat/
Lucent/Orinoco Registry Encr./Decr.	http://www.cqure.net/tools.jsp?id=3
MacStumbler	http://www.macstumbler.com/
MiniStumbler	http://www.netstumbler.com/download.php?op=viewdownload&cid=1
Mognet	http://www.node99.org/projects/mognet/
NetChaser	http://www.bitsnbolts.com/netchaser.html
NetStumbler	http://www.netstumbler.com/download.php?op=viewdownload&cid=1
PocketWarrior	http://www.pocketwarrior.org/ //Pong
PrismStumbler	http://prismstumbler.sourceforge.net/
SSIDsniff	http://www.bastard.net/%7Ekos/wifi/
StumVerter	http://www.sonar-security.com/ //THC-LEAPcracker
void11	http://www.wlsec.net/void11/
WarGlue	http://sourceforge.net/projects/warglue

Wireless Tools (cont.)

WarLinux	http://sourceforge.net/projects/warlinux/
Wavelan Tools	http://sourceforge.net/projects/wavelan-tools/
WaveMon	http://freshmeat.net/projects/wavemon/
WaveStumbler	http://www.cqure.net/tools.jsp?id=08
WellenReiter	http://www.wellenreiter.net/ //WepAttack
WEPCrack	http://sourceforge.net/projects/wepcrack/
Weplab	http://sourceforge.net/projects/weplab
WEPWedgie	http://sourceforge.net/projects/wepwedgie/
WEP_Tools (wep_crack/wep_decrypt)	http://www.lava.net/%7Enewsham/wlan/wep_tools.tgz
Wi-Find	http://evvl.rustedhalo.net/projects/wi-find/
WifiScanner	http://wifiscanner.sourceforge.net/
WinDump	http://windump.polito.it/
WiStumbler	http://www.gongon.com/persons/iseki/wistumbler/index.html
wscan	http://www.cs.pdx.edu/research/SMN/

Demonstration



802.11 Security – The Next Generation

- 802.11i Security
  - 802.11 Working Group introduced strong security
    - 802.11i
  - Temporal Key Integrity Protocol (TKIP)
    - Each station gets a separate key for confidentiality
    - This key is changed frequently

802.11 Security – The Next Generation

- 802.11i Security
  - Products started becoming available in late 2003
- Wireless Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - Introduced some parts of 802.11i in 2002 and 2003

Summary of Recommendations

- Locate the Router or Access Point Appropriately
- Change Default Administrator Passwords
- Change the Default SSID
- Disable SSID Broadcast
- Turn on Encryption
- Enable MAC Address Filtering
- Assign Static IP Addresses to Devices